

WHAT WE CLAIM:

1. A pseudo-random key generator for use within a cryptographic communication system, said pseudo-random key generator comprising:

a pseudo-random number generator; and

a computer readable storage medium connected to said pseudo-random number generator.

2. The cryptographic communication system according to claim 1, further comprising a timing circuit connected to said pseudo-random number generator.

3. The cryptographic communication system according to claim 1, wherein said timing circuit further comprises:

a clock connected to said pseudo-random number generator;

a delta counter connected to said clock; and

a time/key initialize device connected to said delta counter.

4. ~~The cryptographic communication system according to claim 2, wherein said computer readable storage medium includes a PRN re-map table.~~

5. The cryptographic communication system according to claim 1, wherein said computer readable storage medium includes a key block formation table.

6. The cryptographic communication system according to claim 1, further comprising a read only computer readable storage medium connected to said timing circuit.

7. The cryptographic communication system according to claim 6, wherein said read only computer readable storage medium comprises:

a crypto midnight date and time value; and

a key change period value.

The cryptographic communication system according to claim 4, further comprising a systems re-map generator connected to said computer readable storage medium.

8. The cryptographic communication system according to claim 8, wherein said computer readable storage medium includes an executable program, said executable program causing said systems re-map generator to re-map the data of said PRN re-map table.

9. The cryptographic communication system according to claim 8, wherein said systems re-map generator selectively rearranges data stored in said computer readable storage medium.

10. A cryptographic communication system having a pseudo-random key generator, said pseudo-random key generator comprising:

B¹

a pseudo-random number generator;

a timing circuit connected to said pseudo-random number generator;

a first computer readable storage medium connected to said pseudo-random number generator;

a systems re-map generator connected to said first computer readable storage medium;

a second computer readable storage medium connected to said first computer readable storage medium; and

a third computer readable storage medium connected to said timing circuit.

2005-04-25 10:56:00

Self
3

11. The cryptographic communication system according to claim 11, wherein said first computer readable storage medium contains a PRN re-map table.

12. The cryptographic communication system according to claim 11, further comprising a systems re-map generator connected to said first computer readable storage medium, wherein said systems re-map generator selectively rearranges data in said first computer readable storage medium.

13. The cryptographic communication system according to claim 11, wherein said third computer readable storage medium includes:

a key change period value; and

a crypto midnight date and time value.

a³
cont

~~14. The cryptographic communication system according to claim 11, wherein said third computer readable storage medium includes a security fuse.~~

B¹
am⁴

15. A method of pseudo-randomly generating cryptographic keys in a cryptographic communication system having a pseudo-random number generator and a computer readable storage medium, said method comprising the steps of:

inputting into said pseudo-random number generator a unique systems seed value;

generating a pseudo-random numerical value;

generating a first data string using said pseudo-random numerical value; and

generating a second data string using said first data string.

~~16. The method according to claim 16, further comprising the steps of:~~

~~inputting into said computer readable storage medium a key change period value; and~~

~~inputting into said computer readable storage medium a crypto midnight date and time value.~~

17. The method according to claim 17, further comprising the step of initializing said pseudo-random number generator.

Q4
crit

18. ~~The method according to claim 18, further comprising the step of initializing said computer readable storage medium~~

19. A cryptographic communications system comprising a pseudo-random key generator, said pseudo-random key generator comprising:

a pseudo-random number generator;

a computer readable storage medium connected to said pseudo-random number generator; and

a re-map device connected to said computer readable medium.

20. The cryptographic communication systems according to claim 20, further comprising a timing circuit connected to said pseudo-random number generator.

21. A cryptographic communications systems comprising:

a plurality of pseudo-random key generators, each of said pseudo-random key generator comprising:

a pseudo-random number generator;

a timing circuit connected to said pseudo-random number generator;

a first computer readable storage medium connected to said pseudo-random number generator;

a systems re-map generator connected to said first computer readable storage medium;

0057591560

a second computer readable storage medium connected to said first computer readable storage medium; and

a third computer readable storage medium connected to said timing circuit.

*Sub
A5*

22. The cryptographic communications system according to claim 20, wherein each of said pseudo-random key generator includes a unique systems seed value.

051900/1257/28189.00010